Amendments to the Claims

1. (Currently amended) A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method comprising the steps of:

performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device ~~and transferring the digital data from the memory to the receiving device, authenticating devices between the input device and the memory and between the memory and the receiving device respectively~~; and

performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device

~~when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, decrypting the implemented electronic signature so as to transfer the digital data after ensuring that it has not been changed since it was recorded~~.

2. (Currently amended) The method of claim 1 comprising the step of:

mixing data for ~~authenticating devices~~ performing device authentication into the digital data ~~to be~~ written from said input device to said memory device and the digital data ~~to be~~ transferred from said memory device to said receiving device.

3. (Currently amended) The method of claim 1 wherein said second device authentication is performed by a central processing unit built into said memory device ~~comprising the step of:~~

~~implementing by a central processing unit built into said memory authentication between said input device and said receiving device and authentication to the digital data in said memory and decryption of said implemented authentication~~.

4. (Currently amended) The method of claim 1 wherein said digital data is transferred as authenticated data if said first and second device authentications are successful and is transferred as ordinary data if said first and second device authentications are not successful ~~comprising the step of:~~

~~only if authentication between said input device and said memory and between said memory and said receiving device is successful, performing the writing of digital data from said input device to said memory and the transfer of digital data from said memory to said receiving device; and if the authentication is not successful, performing ordinary writing and transfer of digital data.~~

5. (Currently amended) The method of claim 1 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key:~~-~~

~~between said input device and said memory, said system having a specific mutual encryption function Hdc and an internal key Kdc used for authenticating both of them; said memory having a hash function Hcf and an internal key Kcf used for an electronic signature in said memory; and between said memory and said input device, said system having a specific mutual encryption function Hpc and its key Kpc used for authenticating both of them~~.

6. (Cancelled)

7. (Cancelled)

8. (Currently amended) The method of claim 1 wherein said device authentication ~~from~~ between said input device ~~to~~ and said memory device is performed by using a public key system.

9. (Cancelled)

10. (New) The method of claim 1 wherein each of said device authentications involves having a first device ascertain that a second device possesses a secret value corresponding to a value held by the first device.

11. (New) The method of claim 10 wherein the first device is a recipient of digital data from the second device.

12. (New) The method of claim 1 wherein each of said device authentications involves the exchange of an authentication value generated independently of said digital data.

13. (New) The method of claim 1, comprising the further steps, performed by the memory device, of:

generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and

authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

14. (New) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 1.

15. (New) Apparatus for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said apparatus comprising:

means for performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

means for performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

16. (New) The apparatus of claim 15 wherein said means for performing said second device authentication comprises a central processing unit built into said memory device.

17. (New) The apparatus of claim 15 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key.

18. (New) The apparatus of claim 17 wherein said encryption functions and said first key are stored in a read-only memory of said memory device.

19. (New) The apparatus of claim 17 wherein said second key is encrypted and stored in NAND record space.

20. (New) The apparatus of claim 15, further comprising:

means associated with the memory device for generating an electronic signature on digital data when writing the digital data from the input device to the memory device; and

means associated with the memory device for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

21. (New) A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:

means for performing a first device authentication with the input device when writing digital data from the input device; and

means for performing a second device authentication with the receiving device when transferring the digital data to the receiving device.

22. (New) The memory device of claim 21, further comprising:

means for generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and

means for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

23. (New) A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method being performed by said memory device and comprising the steps of:

generating an electronic signature on digital data when writing the digital data from the input device to the memory device; and

authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

24. (New) The method of claim 23 wherein said memory device generates said electronic signature using a hash function and an internal key.

25. (New) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 23.

26. (New) A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:

means for generating an electronic signature on digital data when writing the digital data from the input device;

means for storing the digital data and the electronic signature; and

means for authenticating the electronic signature on the digital data when transferring the digital data to the receiving device.

27. (New) The memory device of claim 26 wherein said means for generating said electronic signature comprises a central processing unit built into said memory device.

28. (New) The memory device of claim 26 wherein said electronic signature is generated using a hash function and an internal key.

29. (New) The memory device of claim 28 wherein said hash function and internal key are stored in a read-only memory of said memory device.

30. (New) The memory device of claim 26 wherein said memory device is a flash memory and stores said electronic signature on said digital data in a redundant area not to be calculated by an ECC of each page in a memory area.